4 statements about science and security

Dusko Pavlovic

Kestrel Institute and Oxford University

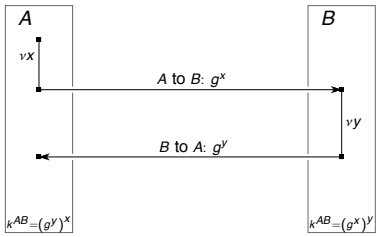
Science of Security Workshop
Oakland, CA
17-18 November 2008

Question

- Why is there no Science of Security?
- Why is security hard to measure?

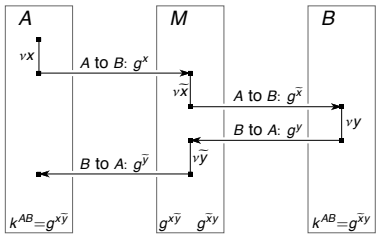
Secure channels on insecure networks

It is easy to set up a secure channel



Secure channels on insecure networks

It is hard to know who you are talking to



What is the problem with authentication?

Why is it that

- encryptions are broken once in a while
- authentications are broken daily?

What is the problem with authentication?

Why is it that

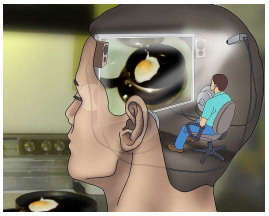
- Shannon's first memo introduced a science
- Shannon's second memo applied it to secrecy
- . . . but it doesn't really apply to authentication?

Authentication is a hard problem for science

Every experiment is concerned with data authenticity.

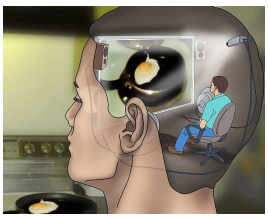
Authentication is a hard problem for science

Derive global facts from local observations



Authentication is a hard problem for science

Derive global facts from local observations



René Descartes: "I think, therefore I exist."

Authentication is a hard problem for science

Derive global facts from local observations

There is no logical impossibility in the hypothesis that the world sprang into being five minutes ago, exactly as it then was, with a population that "remembered" a wholly unreal past.

Bertrand Russell
The Analysis of Mind

Authentication is a hard problem for science

— like the existence of God for religion?

Derive global facts from local observations

There is no logical impossibility in the hypothesis that the world sprang into being five minutes ago, exactly as it then was, with a population that "remembered" a wholly unreal past.

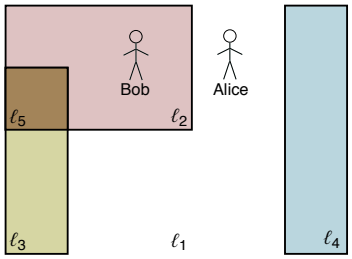
Bertrand Russell
The Analysis of Mind

Statement 1

- **Secrecy is no problem.**
- **Authentication is the problem.**

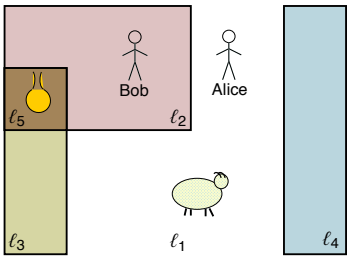
Where does security come from?

About 6000 years ago, Kain's son Bob built a secure vault



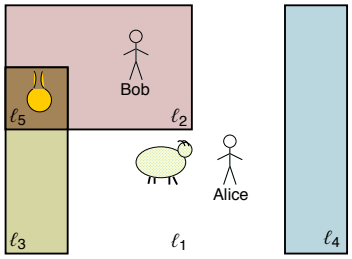
Where does security come from?

and stored his goods in it.



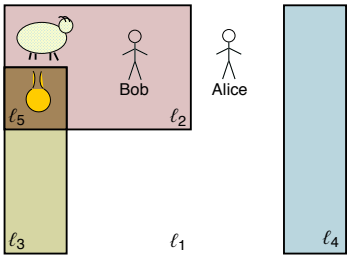
Where does security come from?

and stored his goods in it. When Alice wanted to go for a vacation



Where does security come from?

and stored his goods in it. When Alice wanted to go for a vacation, she stored her goods there too.



Where does security come from?

As a receipt for her deposit in Bob's vault, Alice got a *secure token in a clay envelope*.

Figure: Louvre, Paris

Where does security come from?

As a receipt for her deposit in Bob's vault, Alice got a *secure token in a clay envelope*.

Figure: Louvre, Paris

- To take the sheep, Alice must give the token.

Where does security come from?

As a receipt for her deposit in Bob's vault, Alice got a *secure token in a clay envelope*.

Figure: Louvre, Paris

- To take the sheep, Alice must give the token.
- To give the sheep, Bob must take the token.

Where does security come from?

As a receipt for her deposit in Bob's vault, Alice got a *secure token in a clay envelope*.

Figure: Louvre, Paris

- To take the sheep, Alice must give the token.
- To give the sheep, Bob must take the token.
- Anyone who gives the token can take the sheep.

Where does security come from?

- This protocol goes back to Uruk (Irak), 4000 B.C.
- Money developed from security tokens.
- Numbers developed from security annotations.
- Writing developed later.
- Science developed still later.

Statement 2

Security is older and broader than science.

Security is a social process

- Studying security as a mere technical problem
  - computer security
  - web security
  - airport security
  - . . .

Security is a social process

- Studying security as a mere technical problem
  - computer security
  - web security
  - airport security
  - . . .

  is like
- studying lung diseases as mere physiology
  - ignoring that some people smoke
  - some people grow and sell tobacco
  - some people collect taxes
  - . . .

Statement 3

- **Security-on-its-own is simple.**
- **Security-in-its-social-context is complex.**

Adverse selection

	TRUSTE-certified	uncertified
honest	94.6%	97.5%
malicious	5.4%	2.5 %

Table: Trustworthyness of TRUSTE [Edelman 2007]

Adverse selection

Google		
	sponsored	organic
top	4.44%	2.73%
top 3	5.33%	2.93 %
top 10	5.89%	2.74 %
top 50	5.93%	3.04 %

Table: Malicious search engine placements [Edelman 2007]

Adverse selection

Yahoo!		
	sponsored	organic
top	6.35%	0.00%
top 3	5.72%	0.35 %
top 10	5.14%	1.47 %
top 50	5.40%	1.55 %

Table: Malicious search engine placements [Edelman 2007]

Adverse selection

Ask		
	sponsored	organic
top	7.99%	3.23%
top 3	7.99%	3.24 %
top 10	8.31%	2.94 %
top 50	8.20%	3.12 %

Table: Malicious search engine placements [Edelman 2007]

Adverse selection

"Pillars of the society" phenomenon

- social hubs are more often corrupt
- the rich are more often thieves
- ...

Trust distribution

Theorem

In the long run, the distribution of the number of trustees with trust rating n is

$$w_n \approx C \cdot n^{-\left(1+\frac{1}{e}\right)} \cdot \prod_{\ell=1}^{n} \gamma_\ell$$

where γ_ℓ is the probability that a principal with trust rating ℓ is malicious.

What does this mean?

Trust is like money

If $\gamma_\ell \to 1$ fast enough (the cheaters do not wait too long), then the distribution of trust is scale free.

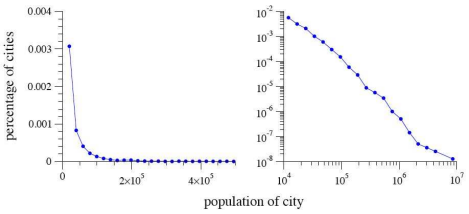


Figure: Power law $w(x) = ax^{-(1+b)}$

What does this mean?

Origin of scale-free distributions

V. Pareto: "The rich get richer"

What does this mean?

Origin of scale-free distributions

V. Pareto: "The rich get richer"

Robustness of scale free distributions

The market is stabilized by the hubs of wealth.

What does this mean?

Origin of scale-free distributions

V. Pareto: "The rich get richer"

Robustness of scale free distributions

The market is stabilized by the hubs of wealth.

Fragility of scale free distributions

Theft is easier when there are very rich people.

Securing trust

Solution

Modify the processes of accumulation of trust to assure a less fragile distribution.

Securing trust

Solution??

Modify the processes of accumulation of trust to assure a less fragile distribution.

Problem

Simple social processes lead to complex security (policy) problems.

Statement 3

- **Security-on-its-own is simple.**
- **Security-in-its-social-context is complex.**

Complexity is relative to the resources

Traveling Salesman Problem

- NP-hard for Turing machines
- ANT-easy in your yard
  - using pheromone as a computational resource

Complexity is relative to the resources

Traveling Salesman Problem

- NP-hard for Turing machines
- ANT-easy in your yard
  - using pheromone as a computational resource

Fermat Theorem

- hard for Andrew Wiles
- easy for Andrew Wiles + community

Compexity itself is a resource

In cyberspace

- authentication is based on secrets
- secrets are based on complexity

Compexity itself is a resource

In cyberspace

- authentication is based on secrets
- secrets are based on complexity

. . . there is more authentication

- René to himself: *"I think, therefore I exist"*
- Alice to Bob: *"Noone else could decrypt this, therefore you exist."*

Public key cryptography

- Whit Diffie and Marty Hellman proposed computational hardness as a new foundation for cryptography in **1976**.
- Ron Rivest, Adi Shamir and Len Adleman (RSA) implemented that idea using exponentiation in **1978**.

Public key cryptography

- Whit Diffie and Marty Hellman proposed computational hardness as a new foundation for cryptography in **1976**.
- Ron Rivest, Adi Shamir and Len Adleman (RSA) implemented that idea using exponentiation in **1978**.
- The RSA patent became a base of a very profitable company.

Public key cryptography

- Whit Diffie and Marty Hellman proposed computational hardness as a new foundation for cryptography in **1976**.
- Ron Rivest, Adi Shamir and Len Adleman (RSA) implemented that idea using exponentiation in **1978**.
- The RSA patent became a base of a very profitable company. All involved became rich and famous.

Non-secret encryption

- In December 1997, the British Government Communications Headquarters (GCHQ) released five papers.

Non-secret encryption

- In December 1997, the British Government Communications Headquarters (GCHQ) released five papers.
- James Ellis' paper *"The possibility of non-secret encryption"* proposed computational hardness as a foundation for cryptography.
- Clifford Cocks' paper *"A note on non-secret encryption"* implemented that idea using exponentiation.

Non-secret encryption

- In December 1997, the British Government Communications Headquarters (GCHQ) released five papers.
- James Ellis' paper *"The possibility of non-secret encryption"* proposed computational hardness as a foundation for cryptography. ⇜ **1970**
- Clifford Cocks' paper *"A note on non-secret encryption"* implemented that idea using exponentiation. ⇜ **1973**

Non-secret encryption

- James Ellis retired in 1986 and died in November 1997.
- Clifford Cocks became the Chief Mathematician at GCHQ in 2007.

Non-secret encryption

- James Ellis retired in 1986 and died in November 1997.
- Clifford Cocks became the Chief Mathematician at GCHQ in 2007.
- Public key cryptography was critical for nonproliferation control as of 1986.

Non-secret encryption

- James Ellis retired in 1986 and died in November 1997.
- Clifford Cocks became the Chief Mathematician at GCHQ in 2007.
- Public key cryptography was critical for nonproliferation control as of 1986. Some say that it expedited the end of Cold War.

Non-secret encryption

I find myself in an embarrassing position, as I have come to doubt the whole theory of non-secret encryption. I have no proof that the method is genuinely secure. . .

The whole field seems hopelessly complex. It would be good to talk to someone who knows more number theory, and to someone who knows more complexity theory. . .

Malcolm Williamson
(proposed the "Diffie-Hellman" key exchange in 1974)

Statement 4

Security through Collaboration
complexity is a resource, not a limitation.[1]

[1] with a nod to the organizers of our collaborative community :)

PS

Science of Security should not only generate innovative technologies, but also innovative social narratives, and even innovative social structures.

Science is an integral part of culture, like religion, art and football. It should speak to people like they do.